TECHNOLOGY UPDATE

"Insider Tips To Make Your Business Run Faster, Easier, And More Profitably"

What's New

B4 Networks welcomes

DESKS PLUS

As their new fully-managed client

IT COMPANIES 50 BEST MANAGED

MSPmentor® 501 2017 WINNER

August 2018

"As a business owner, I know you don't have time to waste on technical and operational issues. That's where we shine! Call us and put an end to your IT problems finally and forever!"

Bryan Lachapelle, B4 Networks Inc.

B4 networks

160 Hwy 20 W. Unit 10
Box 249
Fonthill, Ontario, L0S 1E0
Tel: 905-346-4966

Employees Keeping Your Data Safe? Don't Count On It.

One morning late last year, an unemployed man was making his way across London, heading to the library to continue his job search. But on the way, he encountered something peculiar: a USB stick, peeking out among the fallen leaves and shining in the morning sun. Not thinking much of it – and perhaps afflicted with a morbid curiosity – he popped the device into his pocket and continued on his way. Once he made it to the library, he connected the USB to a computer to check out its contents. As he clicked around, he realized with a shock that this was a treasure trove of security information for the Heathrow International Airport: 174 folders packed with maps detailing CCTV camera locations, labyrinthine tunnels snaking below the building and even the exact route the Queen takes when she uses the airport.

Understandably worried, the man quickly ejected the device and brought it – for some

Continued on pg.2

Continued from pg.1

reason – to local tabloid the *Daily Mirror*. Today, despite a full-scale security investigation by the airport and the scrutiny of dozens of police and security experts, it's still unclear just where this extremely sensitive data came from. However, all signs point to the USB drive being dropped by either a hapless employee carrying around a national security concern in their pocket or a less-hapless employee looking to instigate a national security crisis.

Either way, the story hammers home a vital point: whether you're an international airport hosting more than 70 million travelers each year or a small business with less than $10 million in annual revenue, your biggest security risk isn't some crack team of hackers – it's your employees.

> **"Your biggest security risk isn't some crack team of hackers – it's your employees."**

Sure, you may chuckle at the idea that any of your employees would actively wish your organization harm. But we're willing to guess that you probably underestimate the wrath of an employee scorned. Even if you treat your team better than any boss in the world, they are still human – which, of course, means they're going to make mistakes from time to time. And when considering the cyber security of many SMBs, "time to time" actually means every day, leaving huge openings in your digital barriers. These errors don't much matter, really – until the day that a hacker turns an eye toward your business and immediately realizes the laughable security gaps your team is leaving for them to exploit.

The thing about cyber security is that it's a lot more complicated than most people are willing to admit. Today's digital landscape is fraught with hazards, a thousand little mistakes to be made at every step, resulting in a million workarounds for cyber criminals to use. Even the most tech-savvy among us probably don't know everything about cyber security, and very few have as much knowledge as the hackers on the other end of the equation. When you consider the uncertainty and potential miseducation of

your employees, many of whom probably know next to nothing about cyber security, you might start to feel a little panicked.

The battle against digital threats can seem like an endless slog – a war that the good guys seem to be losing – but luckily, when it comes to the security of your business, there are ways to batten down the hatches without dropping a ton of cash. For instance, start with your biggest vulnerability: your team. When a new employee joins your organization, they should go through a thorough cyber security training. Their welcome forms should include comprehensive rules about security policies, from using strong passwords to how they should respond to potential phishing attempts. Deviating from these policies should come with serious consequences.

As for your existing employees, train them up! We can help you build a robust education program to get every single member of your organization up to speed on the most imminent cyber security threats. But even then, cyber security isn't a one-and-done kind of thing; it requires constant vigilance, regular updates on the latest trends and a consistent overall commitment to protecting your livelihood. Without training and follow-up, even the most powerful of cyber security barriers are basically tissue paper, so put some thought into your team in addition to your protections, and you can drastically increase the safety of the business you've worked so hard to build.

8 Tendencies Of Bad Decision Makers

By Mike Michalowicz

At one point in my career, after I'd started, grown and sold a couple of businesses, I thought I knew everything there was to know about making good decisions. After all, I was a success! But it took me a few years to realize that, in many respects, I still had a lot to learn about making the best calls. Here are the lessons I learned the hard way back then about the tendencies and motivations of people who are making the worst business decisions of their lives.

BASING DECISIONS ON EGO

If you think you know it all and that your expertise in a narrow field will translate to every other field, you're just flat wrong. Assemble a team of folks whose experience rounds out your own and reap the benefits of multiple perspectives.

RELYING ON THE MOMENTUM EFFECT

There's certainly some truth to the belief that past events can predict future events. The problem with this thinking, though, is that the world is constantly evolving. If you're sticking with the tried-and-true and refusing to look at other options, you're likely to misstep.

BEING LAZY

Entrepreneurs have to be hungry and curious. Make sure you're looking at the whole picture, and at both the negatives and positives of any potential decision.

BEING INDECISIVE

If you're putting off making a choice, you can end up limiting your options down the road. You may be right, you may be wrong, but don't let yourself get cheated out of success.

GOING IT ALONE

You simply can't understand all the options and complexities of a given situation on your own. Sometimes the best results come through compromise with a team you've assembled.

EXECUTING POORLY

Making a decision is only 10% of the process. The other 90% is the actual execution of that decision. If you fail to communicate the reasons for your decision to your staff, neglect to plan or follow up, or simply drop the ball, you're not getting the job done. Make sure you implement your changes in a thoughtful, logical way.

SEEING THE TREES RATHER THAN THE FOREST

Good decisions are made with the big picture in mind. If you're focused on putting out fires or only thinking about next week, you're not going to be able to adequately plan ahead. Leave the short-term decisions to your trusted staff and devote your energy to the long term.

NOT BALANCING YOUR SOURCES

Abraham Lincoln was a great president, but it wasn't just because he was a smart, thoughtful man. He surrounded himself with a cabinet comprised of his most bitter rivals, understanding the power of hearing from people other than "yes" men. Don't fall into the trap of listening to sycophants who tell you only what you want to hear. By seeking out contrary opinions, you'll avoid making decisions based on biased sources.

MIKE MICHALOWICZ (pronounced mi-KAL-o-wits) started his first business at the age of 24, moving his young family to the only safe place he could afford – a retirement building. With no experience, no contacts and no savings, he systematically bootstrapped a multimillion-dollar business. Then he did it again. And again. Now he is doing it for other entrepreneurs. Mike is the CEO of Provendus Group. He is also a former small-business columnist for The Wall Street Journal; MSNBC's business makeover expert; a keynote speaker on entrepreneurship; and the author of the cult classic book The Toilet Paper Entrepreneur. His newest book, The Pumpkin Plan, has already been called "the next E-Myth!" For more information, visit www.mikemichalowicz.com.

How Does Your Current I.T. Company Compare?

Our July 2018 Service Key Performance Indicators

87%

8 Business Hour Ticket Resolution

92%

Client Satisfaction

9 mins

Average Response Time

The Top 5 Business Apps To Improve Your Productivity

In the light-speed world of modern business, workers need every bit of help they can get. Luckily, new apps are developed every day that make our lives easier. Here are five of the best:

Documents To Go allows users to open and edit Microsoft Office 2007 files from any smart device. While that may seem a simple task, if your company frequently uses the Office Suite, Documents To Go can make a big difference.

Evernote has been making waves for a few years now with its seamless approach to notetaking and file-keeping. It enables users to upload virtually everything they need to the cloud and is especially useful for those quick thoughts you jot down during key work meetings.

If it's strictly file syncing you need, check out **SugarSync**. A free account gets you 2GB of shared storage between two computers and your phone, accessible from anywhere.

Remember the Milk is one of the premiere apps for to-do listers everywhere, syncing complex lists across multiple platforms with little effort.

And you can't forget **Skype**, perhaps the best tool for cutting down long-distance charges and communicating via chat, video and audio with far-flung colleagues.

LifeWire.com, 5/17/2018

9 Quick Tips To Protect Your Business From Cyber-Attack

Cyber security is more important than ever, but it doesn't have to be complicated.

Just follow these rules and you'll be well ahead of the game:

1. Only use secure networks.
2. Encrypt your data – it's easier than it sounds.
3. Install a strong firewall.
4. Install patches and updates as soon as they become available.
5. Do your research on the most common cyberthreats (you'd better know what phishing is).
6. Develop a company-wide cyber security policy.
7. Make sure your business WiFi router is protected by the WPA2 standard. (Look it up.)
8. Install software that insulates you from malware.
9. Get SSL (Secure Sockets Layer) Certificate Protection, especially if you take payments online.

SmallBizTrends.com, 4/25/2018

Shiny Gadget of the Month

An Indoor, No-Hassle Cookout: The Kenyon City Grill

As we draw close to the end of summer, many of us are stowing our grills in preparation for the cooler months. Others never had a grill in the first place, banned by their lease from ever doing any sort of grilling. Regardless of the reason, pretty much everyone bemoans a grill-free existence, even if it's only for a few months.

Enter the Kenyon City Grill, a handy grill for those of us who need to stay inside to cook up a hot dog or hamburger. With some complicated engineering tricks, the grill can cook anything you throw at it with virtually no smoke, far exceeding the requirements of city fire codes and preventing you from getting smoked out of your kitchen. Its $475 USD price tag may seem a little steep, but consider the convenience of grilling right from your kitchen, all year long – even if you're in an apartment! – and you can quickly see the benefits.

Today’s Security Challenges and How Microsoft Helps Mitigate Them

Today’s workforce is more mobile than ever, which means they can work from virtually anywhere any time, provided they’ve got an internet connection.

While this is great, it presents a whole new spectrum of security challenges as this level of mobility means more opportunities for a security breach. If this doesn’t ring alarm bells in your head, then picture these statistics:

1. The IBM-sponsored Ponemon Institute’s 2017 Cost of Data Breach Study puts the global average cost of a data breach at a whopping $3.6 million. That’s about $141 for every data record. Not to mention that the cost of recovering from a security breach is higher than protecting against one.

2. More than 80 percent of employees use non-approved SaaS (software-as-a-service) apps in their job, leading to hundreds of million records already compromised to date.
3. An attacker can reside within your network for up to 200+ days on average before detection.

What Microsoft is doing to combat security threats
Microsoft’s protection begins with the unique insights that the tech giant amasses through machine learning technology. Machine learning on Microsoft Security works by overlaying separate sets of company data for its Artificial Intelligence (AI) system to monitor. The system measures each dataset against the other using pattern recognition to detect any anomalous activity which it then flags in order to be addressed.

This threat intelligence gathers signals — or indicators — from a broad and in-depth array of sources to help the security graph understand the threat landscape. This means analyzing and learning from data built into products and services such as Windows, Office 365, Hotmail, and Azure from users all over the planet to detect attack trends and intercept new threats before they happen.

That’s data provided by:

- 400 billion emails monthly
- 2 billion devices monthly
- 1 billion cloud queries daily
- 2 million file samples daily

Microsoft also employs threat researchers and analytics systems across its worldwide network to provide a timely and actionable assessment of the threat landscape. This approach means that Microsoft has billions of data points that throw light on various security issues.

The company is constantly learning from every one of these interactions and creating a security graph built on its broad scale, strength of signal, visionary mindset, and vast experience as a global enterprise. Most importantly, they perform ongoing studies of the threat landscape to help understand and mitigate the impact of more sophisticated attacks.

Pillars of Microsoft Security

Microsoft’s approach to security comes down to four simple pillars: Trust, Intelligence, Partnerships, and Platform.

1. Trust
Microsoft believes in the need to trust that your organization, data, and people are protected from security threats.

2. Intelligence
This is about acting on the intelligence that Microsoft gives you from its security-related signals and insights – helping both Microsoft and its users detect threats more quickly.

3. Partnerships
Microsoft is fostering an ecosystem of vibrant partners whose contributions lead to the effective raising of the security bar across the industry. The tech giant believes in working with the industry as a way to take a holistic approach to technology.

4. Platform
Microsoft security is in-built on the company’s platforms, taking a holistic approach to security by looking at it across identity, apps, devices, and data, as well as the security infrastructure. This involves, for instance, harnessing machine learning on integrated applications such as Windows Defender Advanced Threat Protection (ATP) to seamlessly monitor data, detect threats, and eventually contain them before they become a problem. Since all this is done using technology rather than human input, there is little need for employee involvement or related software deployment.

A more targeted approach to threat protection
Because many of today’s organizations have multiple data centers spread across various locations or all over the globe, there are more opportunities for a security breach. This means that an integrated approach to protection would be a less efficient alternative. Microsoft, therefore, encourages the deployment of more targeted products that narrow the focus and guarantee the security of internal business processes.

A good example is the protection that Microsoft offers for emails; a major point of breach targeted by cybercriminals. Here, Office 365 Advanced Threat Protection (which works in the same way as ATP) focuses only on scanning and detecting suspicious activity within emails.

There is also the Threat Explorer in Office 365 Threat Intelligence and Exchange Online Protection that Microsoft uses along with the Office 365 Advanced Threat Protection to create a broader threat visibility. This guarantees faster detection, investigation, and response to email threats.

Conclusion
With its unique approach, Microsoft is always steps ahead of bad actors that threaten your two biggest assets – people and data. Using Microsoft Office 365 means that you’re leveraging these unique capabilities to increase your protection. The beautiful thing about having world-class security is that it ensures your employees have the peace of mind to do their best work that will yield the most productivity for your organization.

Are Your Kids "Bored"?

Here Are Some Easy Ways To Keep Them Entertained This Summer

PLAY HOPSCOTCH
DRAW WITH CHALK
BOTTLE FLIP
WRITE A STORY
DO A PUZZLE
PLAY DRESS UP
BLOW BUBBLES
WALK THE DOG
READ A BOOK
SEARCH FOR COOL ROCKS
HAVE A PICNIC
MAKE A PAINTING
BOARD GAMES
LOOK AT OLD PICTURES
HAVE A LEMONADE STAND
MAKE A TIME CAPSULE
MAKE FOIL JEWELRY
PLAY CHARADES
HAVE A STARING CONTEST
BAKE A TREAT
PAPER AIRPLANE RACE
WATCH A MOVIE
LEARN A MAGIC TRICK
CREATE A SUPERHERO
FIND TOYS TO DONATE
FIND TOYS FOR GARAGE SALE
PLAY TAG
WASH THE CAR
BUILD WITH BLOCKS
MAKE UP A DANCE
RIDE YOUR BIKE
TAKE PICTURES
WASH THE DOG
PLAY FREEZE DANCE
HAVE A TEA PARTY
WATER PLANTS
MAKE A CRAFT
LISTEN TO MUSIC
LOOK FOR LADYBUGS
PICK FLOWERS
WRITE A LETTER
PRACTICE A SPORT
DIG IN THE DIRT
PLAY GO FISH
TAKE A BUBBLE BATH
BE HELPFUL
MAKE SOCK PUPPETS
PUPPET SHOW
DRAW YOURSELF
FASHION SHOW
FACETIME GRANDMA
JUMPROPE

Don't Take Our Word For It . Here's What One Of Our Clients Has To Say About Us:

"Since signing on with B4 I have bragged about them..."

"When you work with someone long enough, your first perceptions are usually confirmed. B4 is no exception, they have proved themselves trustworthy and honest. In all facets of business, not just network integrity. Since signing on with B4 I have bragged about them to other business owners, great staff and always return my queries- no matter how mundane. Keep it up, always a pleasure to interact with them"

Jan VanZanten, Van Zanten Greenhouses Inc

Do You Know Someone That Needs Computer Support?

RECEIVE UP TO
$5000
FOR EACH FRIEND
YOU HAVE
REFERRED TO US.

In our opinion, referrals from very happy clients and their employees are the greatest form of flattery. We love it when you're so pleased with our services, that you're willing to recommend us to other business owners you have a relationship with!

If you know someone who is looking for computer support for their company, you will receive $100 for every referral you send our way.

If your referral becomes one of our managed clients, you will receive a cheque up to the amount of one month of their signed agreement. That could be up to $5000 in your own pocket!

For full details about our referral program and to submit your referral, please visit www.b4networks.ca/referral-program today and get us in contact with your friends today!

August Fun Days of the Month

August 1 • World Wide Web Day
August 2 • Ice Cream Sandwich Day
August 4 • Sisters Day
August 8 • International Cat Day
August 9 • Book Lovers Day
August 16 • Rollercoaster Day
August 17 • Thrift Shop Day
August 22 • Eat a Peach Day
August 23 • Burger Day
August 27 • Global Forgiveness Day
August 30 • Slinky Day
August 31 • Eat Outside Day

Client Spotlight—Frontier Utility Locating Services Inc.

Established in 2006 by Kevin Doyle, a veteran electrical utility technician, Frontier Utility Locating Services has become a trusted source for private utility locates throughout Eastern Canada.

Their goal is to increase excavation safety in the environmental, geotechnical and construction industries. Frontier benefits from years of utility and locate experience to help clients achieve that safe goal.

FRONTIER
UTILITY LOCATING SERVICES INC.

Delivering an added layer of safety and protection for clients staff and property, they provide precision utility detection and location on drilling and excavation projects. With projects as small as scanning one proposed borehole location to complete site facility mapping, Frontier provides due diligence for any excavation work that you perform.

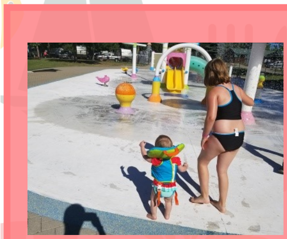
They continue to build on their reputation as a highly-trusted private utility locating firm that is responsive and reliable, helping clients to meet today's rapidly changing safety requirements.

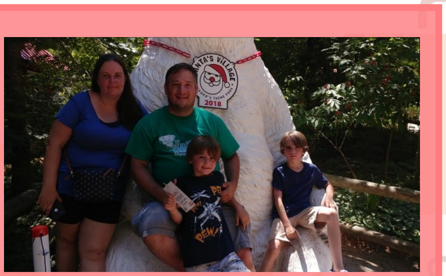
With a thorough understanding of utility installation methods and standards, Frontier delivers a level of experience and knowledge most locate companies don't. Coupled with years of specific service in the environmental, geotechnical and construction industries, they are able to bring these worlds together to provide a comprehensive assessment of your project requirements, and ensure an outstanding level of safety and precaution for each specific job.

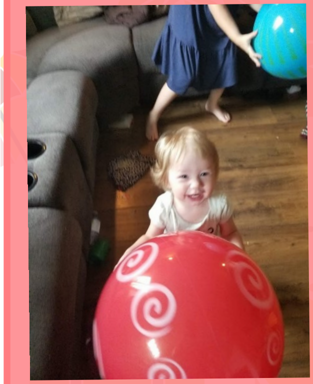
Frontier continues to provide services to an increasingly diverse range of clients and projects, delivering cost-effective and innovative solutions.

Phone: 905-548-7643
Web: www.utilitylocator.ca

PHOTO ALBUM







TEKTIP

Confused About All These Tech Terms?

We've put together a list of terms to provide you with an overall idea of what they mean.

BDR – This abbreviation stands for "backup and disaster recover." This is a plan where all hardware and software is regularly saved in both onsite and offsite locations. This can prevent data from actually being lost.

Cyber or security breach– An internet security breach where cyber thieves hack into your computer systems and steal data or plant malware. These breaches can cripple your organization and damage your data including customer records.

Hybrid Cloud-A cloud computing environment where a mixture of public and private cloud services are created to lower operating costs and gain access to a wider range of computing resources.

IT Infrastructure-This term includes all networking, servers, computers, software, hardware, and other technology used to manage and support all information technology resources.

Malware– A combination of the words "malicious" and "software". This term has come to refer to any type of software that was built for the specific intent of disrupting a company's computer network and damaging computer equipment

Software bug- An error, fault, or flaw in a computer program that produces an unintended effect.

Virtualization- Virtual Machines (VM) are created that look and behave exactly like the real thing. This can include servers, networks, operating systems, or storage devices. This allows a company to have a much more sophisticated IT infrastructure at lower costs.

VPN– Virtual private networks (VPN) are built over public infrastructures to provide a higher level of security to the data transmitted. Usually, encryption is used to protect apps and data from intruders as the data is processed across the internet.